Snort\_dpdk\_mysql环境搭建流程

* + - 1. 安装环境 centos7.0系统

# 宿主机环境搭建

# docker 搭建

# yum install docker-io

1. 更改镜像源如图 更改文件/etc/sysconfig/docker如下



# dpdk搭建

# 获取dpdk源码文件

wget <https://fast.dpdk.org/rel/dpdk-16.04.tar.xz>配置环境变量

1. 更改文件

diff --git a/mk/exec-env/linuxapp/rte.vars.mk b/mk/exec-env/linuxapp/rte.vars.mk

index 5fd7d85..847a3d0 100644

--- a/mk/exec-env/linuxapp/rte.vars.mk

+++ b/mk/exec-env/linuxapp/rte.vars.mk

@@ -41,6 +41,8 @@

#

ifeq ($(CONFIG\_RTE\_BUILD\_SHARED\_LIB),y)

EXECENV\_CFLAGS = -pthread -fPIC

+else ifeq ($(CONFIG\_RTE\_BUILD\_FPIC),y)

+EXECENV\_CFLAGS = -pthread -fPIC

else

EXECENV\_CFLAGS = -pthread

Endif

1. 配置环境变量

RTE\_SDK=dpdk目录

RTE\_TARGET = x86\_64-native-linuxapp-gcc

1. 编译安装

make config T=x86\_64-native-linuxapp-gcc

sed -ri 's,(PMD\_PCAP=).\*,\1y,' build/.config

make install T=x86\_64-native-linuxapp-gcc DESTDIR=/usr/local

# 运行

1. 运行docker容器
2. 构建镜像 进入dpdk\_docker目录

docker build -t [IMAGE NAME] .

1. 构建容器

docker run -it --privileged -v /sys/bus/pci/devices:/sys/bus/pci/devices -v /sys/kernel/mm/hugepages:/sys/kernel/mm/hugepages -v /sys/devices/system/node:/sys/devices/system/node -v /dev:/dev --name [ CONTAINER NAME] [IMAGE ID]

1. 在宿主机构建dpdk环境

进入$RTE\_SDK/tools 利用setup.sh 文件 加载igb\_uio模块 配置大页缓存 和将网卡绑定在igb\_uio模块上

1. 进入容器内部进行snort检测工作
2. 进入/home/test目录
3. Snort检测命令

snort --daq-dir /usr/local/lib/daq/ --daq dpdk -i [dpdk port] --daq-var dpdk\_args="-c 1" -c snort.lua -A u2 -l [log dir] -z [core number snort uses]

1. Barnyard2 命令

Barnyard2 –c barnyard2.conf –d [log dir] –f unified2.log

附录:

# Docker用法简述

Service docker start 启动docker服务

Docker images 察看docker所有镜像

Docker ps 察看docker所有容器

Docker run -it –name [CONTAINER NAME][IMAGE ID] /bin/bash

Docker exec -it [CONTAINER ID] 进入容器

Docker build -t [IMAGES NAME:tag] . 构建镜像

1. Snort2lua用法

Snort2lua -c snort.conf

1. Snort.lua脚本里面有用的参数

本地规则：local\_rules=[[ include rules1 include rules2 ]]

U2日志格式：unified2 = {**legacy\_events=true , limit= , nostamp = false**}

第一项表示是否用snort2.x格式存储日志 true为是 false为否 false是默认值

第二项意义不明 但感觉是日志文件大小

第三项是是否为日志名字加时间戳 true是不加 false是加 true是默认值

1. 服务器网口拓扑图



参考文献 ：

（1）snort3 官方文档

https://snort-org-site.s3.amazonaws.com/production/release\_files/files/000/007/162/original/snort\_manual.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20180820%2Fus-east-1%2Fs3%2Faws4\_request&X-Amz-Date=20180820T173625Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=51c0839180218c1cce445c3e9932cc399a700cc630a2be00e3a58960833443d0

（2）https://blog.csdn.net/nachtz/article/details/52138135?\_t\_t\_t=0.8585992300458676